#31 KW-S 10f3

Attorney Docket No.: 80410.0009

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

MOSKOWITZ, Scott, et al

Appl. No.: 08/999,766

Filed: July 23, 1997

For: STEGANOGRAPHIC METHOD AND DEVICE

Art Unit: 2132

Examiner: MEISLAHN, D.

MAIL STOP: Appeal Brief - Patents
Honorable Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF ON APPEAL

Applicant hereby submits its Brief on Appeal pursuant to 37 C.F.R. § 1.192.

07/11/2003 EGREGAY1 00000075 501129 08999766
03 FC:2403 160.00 DA

07/11/2003 EGREGAY1 00000075 501129 08999766
03 FC:2403 140.00 DA

Respectfully submitted,

WILEY REIN & FIELDING LLP

By: Floyd B. Chapman

Floyd B. Chapman Reg. No. 40,555

Date: July 10, 2003

WILEY REIN & FIELDING LLP
Attn: Patent Administration
1776 K Street, N.W.
Washington, D.C. 20006
Telephone: 202.719.7000
Facsimile: 202.719.7049

Attorney Docket No.: 80410.0009

#31
10f3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

MOSKOWITZ, Scott, et al

Appl. No.: 08/999,766

Filed: July 23, 1997

For: Steganographic Method and Device

Art Unit: 2132

Examiner: MEISLAHN, D.

Honorable Commissioner for Patents
Mail Stop: Appeal Brief-Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

BRIEF ON APPEAL

This is an appeal from the final rejection of claims 25-63, all of the pending claims in the application. Appellant filed its Notice of Appeal on March 10, 2003, and herewith submits its Brief on Appeal in triplicate. The Commissioner is hereby authorized to charge $160.00 (the required filing fee for filing a brief for a small entity) to the deposit account no. 50-1129 of Wiley Rein & Fielding, LLP.

Appellant hereby requests an oral hearing before the Board of Patent Appeals and Interferences. The Commissioner is hereby authorized to charge $140.00 (the required filing fee for requesting an oral hearing for a small entity) to the deposit account no. 50-1129 of Wiley Rein & Fielding, LLP.

The Commissioner is hereby authorized to charge any fees or credit any overpayment to the deposit account no. 50-1129 of Wiley Rein & Fielding, LLP.

REQUEST FOR EXTENSION OF TIME

Applicant respectfully requests a two (2) month extension of time to respond to file its appeal brief in response to its notice of appeal that was filed March 10, 2003, which request will extend the period for response from May 10, 2003 to July 10, 2003. The Commissioner is hereby authorized to charge $205.00 (the required filing fee for a two month extension of time for a small entity) to the deposit account no. 50-1129 of Wiley Rein & Fielding, LLP.

It is believed that no other fees are required to ensure entry and consideration of this response. However, if any fees are required with the filing of this response, Applicants respectfully request that any such fees be charged to Deposit Account No. 50-1129.

Real Party at Interest

This application has been assigned to Wistaria Trading, Inc.

Status of Claims

Claims 1-24 were cancelled, and each of the pending claims 25-63 stands rejected on three independent bases. Appendix A presents a clean copy of the pending claims, and Appendix B includes a claim chart to assist the Board with its analysis.

Status of Amendments

No amendment was filed subsequent to the final rejection

Summary of The Invention

The present invention relates to methods for steganographically protecting digital signals. Claims 25 and 29 are independent method claims, and all other pending claims depend from either Claim 25 or Claim 29.

Generally, the present invention provides a method for steganographically protecting a digital signal. The method provides a carrier signal and uses a stega-cipher (a.k.a., a steganographic cipher) to steganographically encode independent information including a digital watermark into the carrier signal. Specification, pp. 20, 21-22 ("The encoder proceeds in this

manner until a complete copy of the additional information has been encoded in the carrier signal."). The stega-cipher is so named because it uses the steganographic technique of hiding a message in multimedia content, in combination with multiple keys, a concept originating in cryptography. However, instead of using the keys to encrypt the content, the stega-cipher uses these keys to locate the hidden message within the content. Specification, p. 7, ll. 17-20. As described in the specification at page 13, lines 5-11, "[t]he value of the stega-cipher is that it provides a way to watermark the content in a way that changes it slightly, but does not impact human perception significantly."

The present invention also relates to a process for decoding information from signals that have been encoded in accordance with the present invention. The decoding process begins by obtaining a carrier signal that has been encoded with independent information. A stega-cipher is used to decode the independent information including a digital watermark from the carrier signal. The decode process uses the same masks or keys as the encoding process and uses them in the same manner as the encoding process, except that the information is extracted one bit at a time from the carrier signal. Specification, p. 21, ll. 21-22.

Issues

The issues on appeal are as follows:

- Whether claims 25-63 are unpatentable under 35 U.S.C. § 112, first paragraph, as containing subject matter which was not described in the specification to reasonably convey to one skilled in the relevant art that the inventor had possession of the claimed invention.
- Whether claims 25, 27-29, 31-33, 35, 62 and 63 are unpatentable under 35 U.S.C. § 102 over Bender.
- Whether claims 25-33, 35-39, 62 and 63 are unpatentable under 35 U.S.C. § 102 over Powell.
- Whether claims 34, 40-43, 46-48 are unpatentable under 35 U.S.C. § 103 over Powell in view of Schneier.
- Whether claim 34 is unpatentable under 35 U.S.C. § 103 over Bender.
- Whether claims 40-43 and 46-48 are unpatentable under 35 U.S.C. § 103 over Bender in view of Schneier.
- Whether claims 52-57 are unpatentable under 35 U.S.C. § 103 over Powell in view of Barton.
- Whether claims 26, 30 and 52-54 are unpatentable under 35 U.S.C. § 103 over Bender in view of Barton.

Grouping of the Claims

With respect to each of the issues stated above, which applies to a group of two or more claims, the groups of claims stand or fall together, with one exception. With respect to the issue of "Whether claims 34, 40-43, 46-48 are unpatentable under 35 U.S.C. § 103 over Powell in view of Schneier," the claims do not stand or fall together. Instead, claim 34 stands or falls by itself; claims 40-43 and 46-48 stand or fall together.

ARGUMENT REGARDING REJECTIONS UNDER 35 U.S.C. § 112, 1ST PARAGRAPH

A. Section 112 Rejections.

Claims 25-63 stand rejected under 35 U.S.C. § 112, first paragraph, as "containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention." In particular, the Examiner asserts: "There is no teaching of using the watermark to form the key." Office Action dated Dec. 10, 2002, at ¶ 20.

The Examiner has not expressly identified a claim limitation at issue, but it is believed that the Examiner is challenging the claim limitation "stega-cipher" (a.k.a., "steganographic cipher") which appears in each of the independent claims (claims 25 and 29). Because "stega-cipher" did not appear in the original claims, but instead was added by an amendment subsequent to the original filing, it is reasonable to inquire for a written description for the term "stega-cipher."

Because the written description requirement applies to claim language, the written description analysis should focus on the term "stega-cipher"—not on a definition for the term that was requested by an examiner in a subsequent interview. Here, the Examiner has not focused on the claim language, and accordingly, Appellant submits that the Examiner's written description analysis is flawed.

As discussed in detail below, there is no doubt that there is written support for the term "stega-cipher" and accordingly, the rejection for lack of a written description must be overturned. Moreover, even if Appellant is required to show written support for the definition, there is adequate support for the definition as recited, and for this additional reason, the rejection must be overturned.

B. An Analysis Under 112, First Paragraph, Must Assess Whether There Is A Written Description To Support the *Claim Language.*

An analysis under 35 U.S.C. § 112 must focus on the claim language and must assess whether the claim language is supported. *See* MPEP § 2163(II)(A)(3)(b), at 2100-165 ("To comply with the written description requirement of 35 U.S.C. § 112, para. 1, ... each claim limitation must be expressly, implicitly, or inherently supported in the originally filed disclosure") (emphasis added); *see also Martin v. Mayer*, 823 F.2d 500, 505 (Fed. Cir. 1987) ("[The written description analysis] is 'not a question of whether one skilled in the art might be able to construct the patentee's device from the teachings of the disclosure. ... Rather, it is a question whether the application necessarily discloses that particular device.'") (quoting *Jepson v. Coleman*, 314 F.2d 533, 536, 136 U.S.P.Q. (BNA) 647, 649-50 (CCPA 1963)). In this case, the claim limitation at issue is "stega-cipher." Thus, "stega-cipher" must be the focus of a "written description" analysis.

The purpose of the "written description" requirement provides insight and guidance in assessing whether the requirement has been met. The Federal Circuit has found that the purpose of the requirement is to protect against over-reaching claims that may be added by amendment after the filing date:

> Satisfaction of the description requirement insures that subject matter presented in the form of a claim subsequent to the filing date of the application was sufficiently disclosed at the time of filing so that the prima facie date of invention can fairly be held to be the filing date of the application.

Vas-Cath Inc. v. Mahurkar, 935 F.2d 1555 (Fed. Cir. 1991) (quoting *In re Smith and Hubin*, 481 F.2d 914 (CCPA 1973) (citations omitted)). In this case, there can be no doubt that the claim language at issue (stega-cipher) was present in the parent application as originally filed on June 7, 1995, and thus the inclusion of the language in the original filing supports the early filing date. Accordingly, there can be no doubt that the policy behind the written description requirement is met.

It is well settled that "to satisfy the written description requirement, the disclosure as originally filed does not have to provide *in haec verba* support for the claimed subject matter at issue." *Purdue Pharma L.P. v. Faulding Inc.*, 230 F.3d 1320, 1323 (Fed. Cir. 2000) (citing *Fujikawa v. Wattanasin*, 93 F.3d 1559, 1570 (Fed. Cir. 1996)) (emphasis added). The pending

application, however, does provide *in haec verba* support for "stega-cipher." **In fact, "stega-cipher" appears in the original specification no less than 43 times.** In view of this express support, there can be no doubt that the written description requirement is met. *See* MPEP §2163(II)(A)(3)(b), at 2100-165 ("To comply with the written description requirement of 35 U.S.C. § 112, para. 1, ... each claim limitation must be expressly, implicitly, or inherently supported in the originally filed disclosure").

C. **The Introduction of "Stega-Cipher" into the Claims.**

By way of an amendment dated July 25, 2000, Applicant amended claim 25 to recite the use of "a random or pseudo-random key to steganographically encode independent information including a digital watermark into the carrier signal." Response and Preliminary Amendment dated July 25, 2000, at 2. The amended claims were rejected, and in a subsequent interview with the Examiner and the Supervisory Examiner, claims 25 and 29 were discussed and "Language to overcome the rejection of claims 25 and 29 was agreed upon." Interview Summary dated Dec. 13, 2000 (emphasis added). That agreement was to amend the claim language to recite the use of a "steganographic key." After reviewing the specification, Applicant amended the claim language to require "using a stega-cipher [random or pseudo-random key] to steganographically encode independent information including a digital watermark into the carrier signal"; the use of "stega-cipher," as opposed to "steganographic key," was chosen because the term was expressly and repeatedly used in the specification. Response and Amendment dated Jan. 17, 2001, at 1-2. At the time of the amendment, Applicant recited support for the use of a "stega-cipher." *Id.* at 2-3.

Despite the fact that an agreement was reached that overcame the substantive rejections of claims 25 and 29, new rejections issued. It is notable that at that time, the Examiner did not reject the amended claim under 35 U.S.C. § 112, nor did the Examiner make any other rejection to suggest that the term as used in the claim or specification was insufficiently understood. Office Action dated Mar. 27, 2001. Because the application gives sufficient examples for one skilled in the art to understand a "stega-cipher", Applicant should not have to provide any further definition. *See* argument below.

In a subsequent interview, a new Supervisory Examiner expressly required Applicant to recite a definition for "stega-cipher" so that the claims could be discussed in the interview.

Applicant provided a definition,[1] and lengthy discussion entailed. Interview Summary dated December 4, 2001. The Supervisory Examiner also asked for Appellant to identify those passages in the specification that supported the definition, and support was provided. Response dated December 11, 2001. For convenience the written definition is recited below:

> A stega-cipher (a.k.a. a steganographic cipher) is an algorithm or combination of algorithms that performs two functions: (1) a steganographic function to determine where in the carrier signal, data (such as message data or watermark data) can be hidden "in plain view"; and (2) a cipher function that makes use of potential data location information, a random or pseudo random seed, and the message data to generate a key that randomly maps the message data into the carrier signal. The use of the phrase "in plain view" does not limit the claimed invention to visual applications.[2]

Response dated December 11, 2001. The resulting rejection under 112 then issued, but it did not expressly identify which claim limitation was being challenged. Office Action dated April 5, 2002. Because the language of the 112 rejection appears to recite portions of the definition, Applicant believes the 112 rejection is directed to "stega-cipher" and accordingly, Applicant responded by identifying support for "stega-cipher." Response dated October 4, 2002 at 1-5.

D. <u>The Term "Stega-Cipher" Is Described and Supported in the Specification.</u>

The Specification provides extensive, explicit support for "Stega-Cipher." Page 7 of the Specification (at lines 13-25) introduces the term "Stega-Cipher":

> The invention draws on techniques from two fields, cryptography, the art of scrambling messages so that only the intended recipient may read them, and steganography, a term applied to various techniques for obscuring messages so that only the intended parties to a message even know that a message has been sent, thus it is termed herein as a stega-cipher. The **stega-cipher** is so named

---

[1] The language on page 1 of the Interview Summary dated December 4, 2001, makes clear that the Supervisory Examiner required Applicant to set forth a definition for discussion purposes:

> In response to questions of how Stega-cipher is defined, Attorney asserts that a stega-cipher is an algorithm that performs two functions: (1) to determine where in the carrier signal data can be hidden in plain view; and (2) a cipher function which makes use of data location information, the random seed, and the message to determine where to actually and randomly place the message within the carrier signal. The carrier signal is defined as digital data that is being protected.

[2] As explained in the Response dated December 11, 2001, the language of the definition was modified to recite the use of a key and to recite the use of a random or pseudorandom seed.

> because it uses the steganographic technique of hiding a message in multimedia content, in combination with multiple keys, a concept originating in cryptography. However, instead of using the keys to encrypt the content, the stega-cipher uses these keys to locate the hidden message within the content.

Further passages in the Specification elaborate on the meaning and functionality of a Stega-Cipher. For example, the Specification (page 8, lines 7-14) provides:

> The invention disclosed herein combines two techniques, steganography--obscuring information that is otherwise in plain sight, and cryptography--scrambling information that must be sent over unsecured means, in a manner such that only the intended recipient may successfully unscramble it. The net effect of this system is to specifically watermark a piece of content so that if it is copied, it is possible to determine who owned the original from which the copies were made, and hence determine responsibility for the copies. It is also a feature of the system to uniquely identify the content to which it is applied.

The Specification (page 8, line 26 - page 9, line 2 (emphasis added)) provides:

> The invention improves upon the prior art by providing a manner for protecting copyright in the digital domain, which neither steganography or cryptography does. It improves specifically on steganography by making use of special keys which dictate exactly where within a larger chunk of content a message is to be hidden, and makes the task of extracting such a message without the proper key the equivalent of looking for a needle in a haystack.

The Specification (page 9, lines 18-20) provides:

> The invention uniquely identifies every copy of multimedia content made using the invention, composed of digitized samples whether compressed or uncompressed, including but not limited to still digital images, digital audio, and digital video.

In the "Detailed Description" section of the Specification (at page 13, lines 5-11), a "Digital Copyright Stega-Cipher Protocol and the Decode/Encode Program" are described, adding further commentary on a stega-cipher:

> The value of the stega-cipher is that it provides a way to watermark the content in a way that changes it slightly, but does not impact human perception significantly. And, furthermore, that it is made difficult to defeat since one must know exactly where the information resides to extract it for analysis and use in forgery attempts, or to remove it without overly degrading the signal. And, to try to force copyright information one must first be able to analyze the encrypted copyright information, and in order to do that, one must be able to find it, which requires masks.

E. The Specification Supports the Proffered Definition of "Stega-Cipher."

A sample embodiment in the specification provides further support for "stega-cipher." See, for example, Specification at page 18, line 5 through page 24, line 9 (with only the most relevant portions being produced below) (emphasis added):

> III. Example Embodiment of Encoding and Decoding
>
> A modification to standard steganographic technique is applied in the frequency domain described above, in order to encode additional information into the audio signal.
>
> In a scheme adapted from cryptographic techniques, 2 keys are used in the actual encode and decode process. For the purposes of this invention the keys are referred to as masks. One mask, the primary, is applied to the frequency axis of FFT results, the other mask is applied to the time axis (this will be called the convolution mask). The number of bits comprising the primary mask are equal to the sample window size in samples (or the number of frequency bands computed by the FFT process), 128 in this discussion. The number of bits in the convolution mask are entirely arbitrary. This implementation will assume a time mask of 1024 bits. Generally the larger the key, the more difficult it is to guess.
>
> Prior to encoding, the primary and convolution masks described above are generated by a cryptographically secure random generation process. It is possible to use a block cipher like DES in combination with a sufficiently pseudo-random seed value to emulate a cryptographically secure random bit generator. These keys will be saved along with information matching them to the sample stream in question in a database for use in decoding, should that step become necessary.
>
> Prior to encoding, some additional information to be encoded into the signal is prepared and made available to the encoder, in a bit addressable manner (so that it may be read one bit at a time). If the size of the sample stream is known and the efficiency characteristics of the stega-cipher implementation are taken into account, a known limit may be imposed on the amount of this additional information.
>
> ...
>
> Starting with the lowest frequency band, the encoder proceeds through each band to the highest, visiting each of the 128 frequency bands in order. At each band value, the encoder takes the bit of the primary mask corresponding to the frequency band in question, the bit of the convolution mask corresponding to the window in question, and passes these values into a boolean function. This function is designed so that it has a near perfectly random output distribution. It will return true for approximately 50% of its input permutations, and false for the

other 50%. The value returned for a given set of inputs is fixed, however, so that it will always return the same value given the same set of inputs.

If the function returns true, the current frequency band in the current window is used in the encoding process, and represents a valid piece of the additional information encoded in the signal. If the function returns false, this cell, as the frequency band in a given window is called, is ignored in the process. In this manner it is made extremely difficult to extract the encoded information from the signal without the use of the exact masks used in the encoding process. This is one place in which the stega-cipher process departs from traditional steganographic implementations, which offer a trivial decode opportunity if one knows the information is present. While this increases the information storage capacity of the carrier signal, it makes decoding trivial, and further degrades the signal. Note that it is possible and desirable to modify the boolean cell flag function so that it returns true <50% of the time. In general, the fewer cells actually used in the encode, the more difficult they will be to find and the less degradation of content will be caused, provided the function is designed correctly. There is an obvious tradeoff in storage capacity for this increased security and quality.

The encoder proceeds in this manner until a complete copy of the additional information has been encoded in the carrier signal. It will be desirable to have the encoder encode multiple copies of the additional information continuously over the duration of the carrier signal, so that a complete instance of this information may be recovered from a smaller segment of a larger signal which has been split into discontinuous pieces or otherwise edited. It is therefore desirable to minimize the size of the information to be encoded using both compact design and pre-encoding compression, thus maximizing redundant encoding, and recoverability from smaller segments. In a practical implementation of this system it is likely the information will be first compressed by a known method, and then encrypted using public-key techniques, before being encoded into the carrier signal.

The encoder will also prepare the package of additional information so that it contains an easily recognizable start of message delimiter, which can be unique to each encoding and stored along with the keys, to serve as a synchronization signal to a decoder. The detection of this delimiter in a decoding window signifies that the decoder can be reasonably sure it is aligned to the sample stream correctly and can proceed in a methodic window by window manner. These delimiters will require a number of bits which minimizes the probability that this bit sequence is not reproduced in a random occurrence, causing an accidental misalignment of the decoder. A minimum of 256 bits is recommended. In the current implementation 1024 bits representing a start of message delimiter are used. If each sample is random, then each bit has a 50% probably of matching the delimiter and the conditional probability of a random match would be $1/2^{1024}$. In practice, the samples are probably somewhat less than random, increasing the probability of a match somewhat.

In this sample embodiment, it is significant that the number of bits in the primary mask equals the number of elements in each sample window. This permits the stega-cipher to view each of the elements of the sample window as a potential location to encode information. A random seed is fed into a ciphering function (such as DES) to determine which of the potential locations will be used to encode with message content. Finally, the message data itself is part of the key in that it is placed within the carrier data. In other words, the message and the key are entangled in the embedding process because the key determines where the message bits are located. For example, if one were to compare the original (unwatermarked) carrier signal with the watermarked version, you could determine the locations of the message data (*i.e.*, those portions of the key that identify where data is recorded) as well as the content of the message data (*i.e.*, the message data itself). For this reason, you know the key must be at least as long as the message data—or else the complete message could not be embedded into the carrier signal. In this sense, the message (namely, its length) is utilized in determining a key to embed the message.

The Specification (page 26, lines 13-18) further provides:

> An average of 64 bits can be encoded into each window, which equals only 8 bytes. Messages larger than 8 bytes can be encoded by simply dividing the messages up and encoding small portions into a string of consecutive windows in the sample stream. Since the keys determine exactly how many bits will be encoded per window, and an element of randomness is desirable, as opposed to perfect predictability, one cannot be certain exactly how many bits are encoded into each window.

Applicant submits that the original claims as they existed at the time of filing the application also support the definition of stega-cipher. See, for example, original claim 3, pages 39-41 (which discloses how the processor loops through each sample window and utilizes a bit of a random 128 bit primary mask and a bit of a random 1024 bit convolution mask to calculate an offset into a stega-cipher map truth table, and encodes a bit of the message data into the sample when the map function is true).

Finally, Applicant submits that the pseudo-code submitted in the appendix to the application (pages 54-64) also supports the definition of stega-cipher (disclosing how the processor loops through each sample window and utilizes a bit of a random 128 bit primary mask and a bit of a random 1024 bit convolution mask to calculate an offset into a stega-cipher map function, and encodes a bit of the message data into the sample when the map function is true).

In view of the foregoing, appellant submits that the term "stega-cipher" is fully supported by the specification, and Appellant requests that the rejection under 35 U.S.C. § 112 be reversed.

ARGUMENT REGARDING REJECTIONS UNDER 35 U.S.C. §§ 102 AND 103

A. The Examiner Appears to Have Misread Bender.

In the Office Action, the Examiner pointed out that Bender distinguishes steganography from encryption. Office Action dated Dec. 10, 2002, at ¶ 22. The key distinction lies in whether the perceptible characteristics of the underlying data are changed. Steganography seeks to hide a message into the underlying data without changing its perceptible characteristics (*i.e.*, "hide the message in plain view"). Encryption seeks to change the underlying data so that it is no longer recognizable.

Examiner's comments regarding Bender and certain other references suggest that the Examiner has misinterpreted the references. For example, Examiner states several times that "Bender et al. teaches encrypting digital watermarks into information with a key." *See* Office Action dated Dec. 10, 2002, at ¶¶ 30, 31, 32, 33, 34 and 35.

This assertion is inaccurate. It may be fair to characterize Bender to teach encoding watermarks into information, but Bender does not teach "encrypting watermarks into information"—much less "encrypting watermarks into information with a key." Because the Examiner's phraseology is also inconsistent with the language of Bender, it is not entirely clear how the Examiner is construing Bender, especially since the Examiner fails to relate the techniques taught by Bender to the step of "encrypting watermarks into information with a key."

B. The Examiner Appears To Have Misread Powell.

In the Office Action, the Examiner acknowledges the distinction between steganography and encryption, Office Action dated Dec. 10, 2002, at ¶ 22, but the Examiner then appears to overlook the distinctions. The key distinction lies in whether the perceptible characteristics of the underlying data are changed. Steganography seeks to hide a message into the underlying data without changing its perceptible characteristics (*i.e.*, "hide the message in plain view"). Encryption seeks to change the underlying data so that it is no longer recognizable.

In particular, the Examiner's comments regarding Powell and certain other references suggest that the Examiner has not appreciated the distinction between steganography and encryption. For example, Examiner states several times without any detailed explanation that Powell teaches "encrypting digital watermarks into information with a key." *See* Office Action dated Dec. 10, 2002, at ¶¶ 25, 26, 27, and 29. This assertion is inaccurate. It may be fair to characterize Powell to teach encoding "signatures"[3] into a carrier signal (*see, e.g.,* Powell, Abstract, which states "A method and system for embedding signatures within visual images"), but Powell does not teach "encrypting watermarks into information"—much less "encrypting watermarks into information with a key." Because the Examiner's phraseology also is inconsistent with the language of Powell, it is not entirely clear how the Examiner is construing Powell, especially since the Examiner fails to relate the techniques taught by Powell to the step of "encrypting watermarks into information with a key."

C. The Examiner's *Post Hoc* Attempt to Correct His Misreading of Bender and Powell Is Unsatisfactory.

Though Applicant articulated several times that the Examiner had misread the references, the Examiner did not address the argument until the most recent Office Action, stating the following:

> [T]he concept of "encrypting" watermark data into a carrier signal as done by Powell et al. and Bender et al. will from hereon be read as meaning that the watermark data is embedded into a carrier signal using techniques derived from cryptography and steganography.

Office Action dated Dec. 10, 2002, at ¶ 11. This *post hoc* justification is entirely unsatisfactory because it demonstrates that the Examiner is construing Bender and Powell based entirely upon the teachings of the present invention. For example, there is no passage in Powell or Bender that describes embedding a watermark using techniques derived from cryptography and steganography. Once again, the Examiner is merely taking the key words from Applicant's teaching and wrongly crediting them to the prior art.

---

[3] Please note that the "signatures" described in Powell are not cryptographic signatures within the meaning of cryptography, nor are they stega-cipher type signatures within the context of Applicant's invention.

ARGUMENT REGARDING REJECTIONS UNDER 35 U.S.C. § 102

A. Whether claims 25, 27-29, 31-33, 35, 62 and 63 are unpatentable under 35 U.S.C. § 102 over Bender.

Claims 25, 27-29, 31-33, 35, 62 and 63 stand rejected as allegedly anticipated by Bender. *See* Office Action of December 10, 2002, at ¶22. The entirety of the examiner's support for these Section 102 rejections is as follows:

> In their introduction on page 164, Bender et al. distinguish between data hiding and encryption. They also state that hidden data should be "invisible" or inaudible", which meets the limitations of claims 62 and 63. In the first paragraph of the next page, they say that watermarks are one type of data often inserted into files. In section 3.4, which studies spread spectrum environments, a pseudo-random key used to hide information is disclosed. The key, a carrier wave, and data are all combined. In section 1.2 Bender is mentioned as encrypting the embedded data. A reading of the section cited as support for the amendment of 17 January 2001 seems to say that this feature is not inherent to a stega-cipher, but is not quite entirely clear.

Office Action of December 10, 2002, at ¶22.

In order for a reference to anticipate a claim, the reference must disclose each and every element of the claimed invention. Independent claim 25 recites, inter alia, "using a stega-cipher to steganographically encode independent information including a digital watermark into the carrier signal...." Independent Claim 29 contains similar language. The Section 102 rejection based on Bender is improper for at least the reason that Bender fails to disclose the use of a stega-cipher as required by the rejected claims.

The "key" allegedly disclosed in Bender (see Bender, p. 171) is not the same as a stega-cipher used to steganographically encode independent data into a carrier signal within the meaning of the present claims. In fact, there are several differences between a stega-cipher as used in the present invention, and the alleged "key" described in Section 3.4 of Bender. As stated in Bender:

> In [Direct Sequence or "DS"], a "key" is needed to encode the information and the same "key" is needed to decode it. The key is pseudo-random noise that ideally has flat frequency response over the frequency range, *i.e.*, white noise. The key is applied to the coded information to modulate the sequence into a spread spectrum sequence.

Bender at 171. Spread spectrum "is designed to encrypt a stream of information by spreading the encrypted data across as much of the frequency spectrum as possible." Bender at 171. Spread spectrum spreads the encrypted data across the spectrum by using a "key" that has "maximum randomness and flat frequency spectrum." Bender at 172. Bender's "chip" or so-called "key" "is a pseudo-random sequence modulated at a known rate." Bender at 171. This is very different than the stega-cipher of the present invention. A stega-cipher is not a pseudo-random sequence modulated at a known rate.

As disclosed in the specification the "stega-cipher" borrows from both steganography and encryption:

> The invention draws on techniques from two fields, cryptography, the art of scrambling messages so that only the intended recipient may read them, and steganography, a term applied to various techniques for obscuring messages so that only the intended parties to a message even know that a message has been sent, thus it is termed herein as a stega-cipher. The stega-cipher is so named because it uses the steganographic technique of hiding a message in multimedia content, in combination with multiple keys, a concept originating in cryptography. However, instead of using the keys to encrypt the content, the stega-cipher uses these keys to locate the hidden message within the content. The message itself is encrypted which serves to further protect the message, verify the validity of the message, and redistribute the information in a random manner so that anyone attempting to locate the message without the keys cannot rely on pre-supposed knowledge of the message contents as a help in locating it.

Patent Application, p. 7, lines 13-25. Basically, the steganographic portion of the stega-cipher seeks to identify locations within the carrier signal where information may be stored, but it is the cipher portion of the stega-cipher that determines which of those identified locations actually will be used. If all of the locations are used, then it will be easier for others to remove the encoded information, because you can run similar algorithms to identify the candidate locations. The cipher portion uses a mask to encode the independent data into those identified areas, such that not all of the available locations are used. Hence, a hacker will have to wipe out all or almost all of the identified areas to remove the watermark (or simply guess at the potential locations), which generally will degrade the quality of the carrier signal significantly. Bender's key has no such masking; in short, Bender's "key" is not ciphered in any manner, but is simply a pseudo-random sequence based on the white noise inherent to the signal. Accordingly, Bender's "chip" is not a "stega-cipher" within the meaning of the claims.

Moreover, there are differences in how the present invention and how Bender's system detect and read the respective encoded information. Bender's system requires that the "key stream for encoding is known by the receiver" and, in addition, the "following parameters are known by the receiver: chip rate, data rate, carrier frequency, and the data interval." (Bender at 172. This is a lot of information that must be known to decode the encoded data. In the present invention, one only needs a stega-cipher, and more particularly, the key associated with the stega-cipher, to decode. Accordingly, the stega-cipher presents a significant advantage over Bender's "chip."

A stega-cipher, unlike spread spectrum, seeks to maximize the imperceptibility by limiting the number of bits being encoded. This is antithetical to spread spectrum's adding white noise because to encode data as flat spectrum noise requires significantly more data to be encoded. This point is evidenced by the differences between the seeding of Bender's "chip" and the seeding of a stega-cipher of the present invention. Bender's "chip" is a pseudo-random sequence modulated at a known rate." Bender at 171. Each bit in Bender's chip is encoded into the signal, whereas with a stega-cipher, only select bits are encoded. Moreover, with a stega-cipher, it is possible, and indeed likely, that encoding the identical data into the same carrier data will yield a completely different result because the randomness is likely to choose different locations for embedding the data of the watermarks. The inclusion of a "cipher" function, therefore, achieves a different result from that contemplated by Bender.

Because Bender fails to disclose a "stega-cipher" as required by claims 25 and 29, the Section 102 rejection of 25 and 29 must be reversed. Moreover, for the same reasons that claims 25 and 29 are patentable over Bender, the claims that depend from claims 25 and 29 are also patentable over Bender. Applicant requests the Board reverse the Section 102 rejection based on Bender, and allow all of the pending claims.

B. Whether claims 25-33, 35-39, 62 and 63 are unpatentable under 35 U.S.C. § 102 over Powell.

Claims 25-33, 35-39, 62 and 63 stand rejected as allegedly anticipated by Powell. *See* Office Action of December 10, 2002, at ¶23. The entirety of the examiner's support for these Section 102 rejections is as follows: "See page 4, lines 4 and 40-42." Office Action of December 10, 2002, at ¶ 23. For convenience, the cited portions of Powell are reproduced as follows:

> Relative extrema are preferred signature points for two major reasons. First, they are easily located by simple, well known processing. Second, they allow signature points to be encoded very inconspicuously.
> * * *
> Using the Difference of Averages technique or other known techniques, a large number of extrema are obtained, the number depending on the pixel density and contrast of the image. Of the total number of extrema found, a preferred embodiment chooses 50 to 200 signature points. This may be done manually by a user choosing with the keyboard 16, mouse 18, or other pointing device each signature point from among the extrema displayed on the display monitor 14. The extrema may be displayed as a digital image with each point chosen by using the mouse or other pointing device to point to a pixel or they may be displayed as a list of coordinates which are chosen by keyboard, mouse, or other pointing device. Alternatively, the computer 12 can be programmed to choose signature points randomly or according to a preprogrammed pattern.

Powell, p. 4, lines 3-4, and 34-42.

The Examiner has failed to set forth a case of anticipation. The passage cited by the Examiner merely describes that signature points may be chosen 1) by identifying relative extrema points, or 2) randomly. This is insufficient to describe the relevance of the Powell reference to the claims. *See* 37 C.F.R. § 1.104(2) ("In rejecting claims for want of novelty or for obviousness, the examiner must cite the best references at his or her command. ... The pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified.").

In order for a reference to anticipate a claim, the reference must disclose each and every element of the claimed invention. Independent claim 25 recites, inter alia, "using a stega-cipher to steganographically encode independent information including a digital watermark into the carrier signal ...." Independent Claim 29 contains similar language. The Section 102 rejection based on Powell is improper for at least the reason that Powell fails to disclose the use of a stega-cipher as required by the rejected claims.

Powell does not disclose the use of a stega-cipher as claimed by the present invention for at least the following reasons: 1) Powell does not disclose the use of a cipher; 2) Powell does not disclose the use of a key to encode or decode; 3) Powell does not embed independent data into a carrier signal; and 4) Powell does not disclose a relationship between the message, signal and key or cipher. In particular, Powell does not disclose the use of a cipher function that makes use of potential data location information, a random or pseudo random seed, and the message data to generate a key that maps the message data into the carrier signal. Powell does suggest that a

computer "can be programmed to choose signature points randomly or accordingly to a predetermined pattern," Powell, page 4 lines, 40-42, but this is not the same as using a cipher to identify which extrema will be used.

Moreover, Powell does not utilize any key—which is why the "image signature" can only be retrieved through the use of the original, unaltered image. Powell, page 5, line 51-page 6, line 9. The present invention's use of keys to encode also permits the use of keys to decode, resulting in a significant practical difference between Powell's teachings and those of the present invention. The Examiner has ignored this very significant practical distinction. Since an object of the present invention is to protect the original data, it is undesirable (and, indeed, very risky) to circulate unwatermarked copies of the original data for decoding purposes. Circulation of the decode key, rather than the original data, helps to protect the original data from the risk of unauthorized and untraceable copying. For this additional reason, Applicant's invention teaches away from Powell.

Finally, Powell does not embed independent data into the digital image as required by the claimed invention. In Powell, the pixel value (which is a luminance value) is adjusted a small positive or negative amount (preferably 2% to 10% of the initial pixel value), whereby the difference is indicative of a "1" or a "0". (Powell, page 4 lines 42-48). Hence, Powell teaches replacing a pixel value with a new value that is dependent upon the initial value (adjusted upwards or downwards 2-10%) of the pixel value. If the value were not dependent upon the initial value, the embedding would not be inconspicuous. Therefore, for at least this additional reason, Powell is distinguishable.

Because Powell does not disclose the use of a "stega-cipher" as required by each of the rejected claims, the rejection is improper. With respect to claim 29 (and each of claims 30-33 and 35-38 that depend from claim 29), the Section 102 rejection is improper for the additional reason that Powell does not disclose the use of a key to decode any embedded information. In each "preferred" embodiment, Powell requires a comparison of a modified version of an image to the original version of an image, in order to recover any embedded data. This clearly teaches away from using a key. Moreover, as discussed above, since an object of the present invention is to protect the original data, it is undesirable (and, indeed, very risky) to circulate unwatermarked copies of the original data for decoding purposes. Circulation of the decode key, rather than the original data, helps to protect the original data from the risk of unauthorized and untraceable

copying. For this additional reason, Applicant's invention teaches away from Powell, and the rejection of claim 29 and its dependencies is improper.

Applicant requests the Board reverse the Section 102 rejection based on Powell, and allow all of the pending claims.

Argument Regarding Rejections Under 35 U.S.C. § 103

In order to "establish a prima facie case of obviousness, three basic criteria must be met." MPEP § 7.06.02(j). First, there must be some motivation or suggestion to modify the reference or to make the proposed combination. Second, there must be a reasonable expectation of success. "The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on the applicant's disclosure." MPEP § 2142 (citing In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)). Third, the combined references must teach or suggest all claim limitations.

The Examiner has failed to establish a prima facie case of obviousness to the extent that there is no motivation or suggestion to make the proposed combinations of the references as directed by the Examiner. More particularly, there is no motivation to combine Bender with Schneier and/or Barton. Similarly, there is no motivation to combine Powell with Barton and/or Schneier.

According to the MPEP,

> [i]n order to support a conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention obvious in light of the teachings of the references.

MPEP 2142 (citing Ex parte Clapp, 277 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985)) (emphasis added). Further, "[w]hen the motivation to combine the teachings of the references is not immediately apparent, it is the duty of the examiner to explain why the combination of teachings is proper." MPEP 2142 (citing Ex Parte Skinner, 2 USPQ2d 1788 (Bd. Pat. App. & Inter. 1998)).

The Federal Circuit has recently emphasized the importance of providing evidence of motivation to combine in *Winner Int'l Royalty Corp. v. Ching-Rong Wang*, 202 F. 3d 1340, 1348-49 (Fed. Cir. Jan. 27, 2000). "Although a reference need not expressly teach that the disclosure contained therein should be combined with another . . . the showing of combinability, in whatever form, must nevertheless be 'clear and particular.'" *Winner*, 202 F. 3d at 1348-49 (citations omitted). Further, the "absence of such a suggestion to combine is dispositive in an obviousness determination." *Gambro Lundia AB v. Baxter Healthcare Corp.*, 11 F.3d 1573, 1579 (Fed. Cir. 1997).

Applicant submits that the Examiner has not satisfied his initial burden of providing "clear and particular" evidence of motivation to combine for any of the proposed combinations of references. Instead, it appears that the Examiner has simply identified references that allegedly disclose the elements of the claim, and has combined them. Even assuming arguendo that the references contained all elements of the claimed invention, it is still impermissible to reject a claim as being obvious simply "by locating references which describe various aspects of a patent applicant's invention without also providing evidence of the motivating force which would impel one skilled in the art to do what the patent applicant has done." *Ex parte Levengood*, 28 USPQ2d 1300, 1303 (Bd. Pat. App. & Inter. 1993) (emphasis added).

As discussed below, there is no sufficient teaching or suggestion for combining the references as the Examiner has combined them. There is no reasonable expectation of success in combining the references as suggested by the Examiner. Finally, the references, when combined, fail to yield the claimed inventions. For at least these reasons, the Section 103 rejections of Claims 26, 30, 34, 36-63 must be reversed.

A. None of the Cited References Discloses the "Stega-cipher" Limitation.

The Examiner has failed to establish a prima facie case of obviousness for each and every one of the 103 rejections because the cited references, either alone or in combination, fail to disclose all of the claimed elements. All of the Examiner's Section 103 rejections are based in whole or in part upon Bender or Powell. A review of the Examiner's rejections makes clear that in each rejection, the Examiner is relying solely upon Bender or Powell for those elements that are present in the independent claims; the Examiner relies upon the secondary and tertiary references for the elements that are added in the dependent claims.

Noticeably absent from the Examiner's 103 rejections is any discussion whatsoever of the claimed invention's use of a stega-cipher. This confirms that the Examiner is relying upon Bender or Powell (as discussed in connection with the Examiner's 102 rejections) to provide the stega-cipher claim element. As discussed above in connection with the Section 102 rejections, neither Bender nor Powell discloses the use of a "stega-cipher" as required by the independent claims in the application (namely, claims 25 & 29). For at least this reason, the Examiner has failed to establish a prima facie case of obviousness for all claims that depend from Claims 25 and 29. *See* MPEP § 2143.03 ("If an independent claim is nonobvious under 35 U.S.C. § 103, then any claim depending therefrom is nonobvious.") (quoting In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)); *see also* MPEP § 7.06.02(j) (the combined references must teach or suggest all claim limitations). Thus, the Section 103 rejections of all dependent claims (namely, claims 26-28 and 30-63) must be reversed for at least this reason.

B. Whether claims 34, 40-43, and 46-48 are unpatentable under 35 U.S.C. § 103 over Powell in view of Schneier.

1. Powell Cannot Properly Be Combined with Schneier.

There is no motivation to combine Powell with Schneier. The Examiner relies on Schneier's discussion of DES. DES is an encryption standard. Powell purports to relate to data hiding (*i.e.*, steganography) because it seeks to inconspicuously embed signature points in a digital image. Absent the hindsight gained by Applicant's invention, there is no motivation to combine the DES of Schneier with the data hiding techniques of Powell. Equally important, it is not readily apparent that there is a reasonable likelihood of success in combining these two techniques, at least as suggested by Examiner. Powell is seeking to achieve a minimally changed image, whereas DES is seeking to encrypt the image. Applying DES to Powell would logically result in an encrypted image (in contravention of the teachings of Powell). Hence, Powell teaches away from Schneier. Because the Examiner has failed to establish a motivating force and has failed to establish a reasonable likelihood of success, the rejection of claims 34, 40-43, and 46-48 based on the combination of Powell and Schneier must be reversed. *See* MPEP § 2142 (citing In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991) ("The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on the applicant's disclosure.")).

2. The Combination of Powell and Schneier Does Not Disclose the Claimed Inventions.

The Examiner asserts that claims 34, 40-43, and 46-48 are unpatentable over Powell in view of Schneier.[4] Office Action of December 10, 2002, at ¶ 25. The entirety of the Examiner's arguments that claims 34, 40-43, and 46-48 are unpatentable over Powell in view of Schneier is as follows:

> Powell et al. teaches encrypting digital watermarks into information with a key. They do not say that mask sets are used.
>
> Chapter 10 of Schneier deals with the Digital Encryption Standard. DES uses an effectively 56-bit key. As described on pages 224-226, this key is broken down and permuted into the encryption of block data. The key breakdown and the subsequent permutation correspond to applicant's mask set. DES uses starting vectors and padding at the end of messages. These correspond to the start of message delimiter and number of bytes to follow the message of [Applicants'] claims 42 and 47. Claims 43 and 48 are anticipated by DES' mixing of the two 32-bit blocks and the integration of the key. It would have been obvious . . . to encrypt the key-encrypted watermark data of Schneier with DES because DES is an encryption standard.
>
> Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use mask sets to protect data.

Office Action of December 10, 2002, at ¶ 25.

DES is an encryption standard; DES is not the same as steganographic ciphering. DES processes data without regard to the perceptibility of the data, and so, the end result is an encrypted data output that looks nothing like the input. DES does not involve hiding a watermark into independent data, but rather taking the independent data and modifying it to the point that it no longer resembles its initial appearance. This is plainly different from steganography, which relates to the art of hiding something in plain view.

As discussed above, Powell does not teach "encrypting digital watermarks into information with a key." Even if one were to apply DES to the teachings of Powell,[5] it would

---

[4] Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (1994).

[5] After mentioning Powell in the opening premise, the Examiner does not refer to Powell again in paragraph 25 of the Office Action. It may be that the reference to "key-encrypted watermark data of Schneier" was

not yield the claimed invention. Applying DES to Powell would logically result in an encrypted image that plainly is not the same as the claimed invention of using a stega-cipher to steganographically encode a watermark into a carrier signal. Moreover, it would appear that encrypting the image is contrary to the teachings of Powell, which states that signature points should be encoded "very inconspicuously." *See, e.g.,* Powell, p. 4, line 4. Accordingly, the combination fails to disclose the use of a "stega-cipher" as required by the claims. For at least this reason, the Examiner has failed to establish a prima facie case of obviousness. *See* MPEP 7.06.02(j) (the combined references must teach or suggest all claim limitations).

Further, there is no "mask set" in a DES cipher. Contrary to the Examiner's assertion, the key breakdown and permutations are simply data, and bear little relationship, if any, to the mask set claimed in the present application. Accordingly, Applicants traverse the Examiner's assertion that the "key breakdown and subsequent permutations correspond to applicant's mask set." *Id.*

The Examiner has simply failed to establish a prima facie case of obviousness. Moreover, the conclusion that the Examiner reaches, namely, "it would have been obvious ... to use masks to protect data" does not appear to be directed to the claim language. The claimed invention requires the use of a stega-cipher to steganographically encode a watermark into a carrier signal. For the simple reason that combining Powell with DES would result in an encrypted image, it is clear that the result is not a steganographically-encoded watermark, as required by each of the rejected claims. This practical distinction confirms that the combination cannot yield the claimed invention. Moreover, the combination does not utilize a mask set as required by claims 40-51. For at least these independent reasons, Applicant requests the Board reverse the rejections based on the combination of Powell and Schneier.

C. Whether claim 34 is unpatentable under 35 U.S.C. § 103 over Bender.

The Examiner asserts that Claim 34 is unpatentable over Bender. The entirety of Examiner's arguments that Claim 34 is unpatentable over Bender is as follows:

> Bender et al teaches encrypting digital watermarks into information with a key. He does not say that the information is then modified. Encryption modifies data. Official notice is taken that encrypting information in order to protect the

---

intended to be a reference to Powell, but for the same reasons discussed in the main text, the result does not change the fact that the combination does not yield the claimed invention.

> data from unauthorized viewing is old and well-known. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to protect the watermarked data of Bender et al. by encrypting it.

Office Action of December 10, 2002, at ¶ 31. The Examiner asserts that Claim 34 is obvious in view of Bender, yet the basis provided for this assertion does not appear to be related to Claim 34. *See id.* Examiner asserts that "it would have been obvious to a person of ordinary skill in the art at the time the invention was made to protect the watermarked data of Bender et al. by encrypting it." *Id.* Claim 34 is directed, in part, to "modifying the first derivative encoded signal" that was initially referenced in Claim 33. The arguments articulated by the Examiner in ¶ 31 do not appear to be directed to claim 34. For this reason, Examiner has failed to establish a prima facie case of obviousness. Moreover, because Bender fails to teach or suggest "generating a first derivative encoded signal" as referenced in Claim 33 and 34, the rejection based on Section 103 is improper. For this additional reason, Applicant requests that the Section 103 rejection of claim 34 be reversed.

Furthermore, claim 34 is patentable over the combination because the combination fails to disclose the use of a "stega-cipher" as required by the claims. For at least this additional reason, the Examiner has failed to establish a prima facie case of obviousness. See MPEP 7.06.02(j) (the combined references must teach or suggest all claim limitations).

D. <u>Whether claims 40-43, 46-48 are unpatentable under 35 U.S.C. § 103 over Bender in view of Schneier.</u>

1. Bender Cannot Properly Be Combined with Schneier.

There is also no motivation to combine Bender with Schneier. The Examiner relies on Schneier's discussion of DES. As explained above, DES is an encryption standard. Bender purports to relate to data hiding (*i.e.*, steganography). (See the Title and Abstract to Bender). Absent the hindsight gained by Applicant's invention, there is no motivation to combine the DES of Schneier with the data hiding techniques of Bender. Equally important, it is not readily apparent that there is a reasonable likelihood of success in combining these two techniques, at least as suggested by Examiner. If Bender is trying to achieve steganography, it is not readily

apparent how Bender would utilize DES in a steganographic manner.[6] Applying DES to Bender would logically result in an encrypted signal (in contravention of the teachings of Bender). Moreover, using DES to create an encrypted signal is not the same as the claimed invention of using a stega-cipher to steganographically encode a watermark into a carrier signal. Because the Examiner has failed to establish a motivating force and has failed to establish a reasonable likelihood of success, the rejection of claims 40-43 and 46-48 based on the combination of Bender and Schneier must be reversed.

2. The Combination of Bender and Schneier Does Not Disclose the Claimed Inventions.

Examiner rejects claims 40-43 and 46-48 as unpatentable over Bender in view of Schneier. *See* Office Action dated Dec. 10, 2002, at ¶ 35. In addition to the reasons stated above, Applicant submits that this rejection is improper because the combination of Bender and Schneier does not yield the claimed invention.

The Examiner relies on Schneier's discussion of the Digital Encryption Standard as follows:

> Chapter 10 of Schneier deals with the Digital Encryption Standard. DES uses an effectively 56-bit key. As described on pages 224-226, this key is broken down and permuted into the encryption of block data. The key breakdown and the subsequent permutation correspond to applicant's mask set. DES uses starting vectors and padding at the end of messages. These correspond to the start of message delimiter and number of bytes to follow the message of [Applicants'] claims 42 and 47. Claims 43 and 48 are anticipated by DES' mixing of the two 32-bit blocks and the integration of the key. It would have been obvious . . . to encrypt the key-encrypted watermark data of Schneier with DES because DES is an encryption standard.

Office Action dated Dec. 10, 2002, at ¶ 35.

DES is an encryption standard; DES is not the same as steganographic ciphering. DES processes data without regard to the perceptibility of the data, and so, the end result is an

---

[6] Note that the present application does recite that DES may be used with the present invention, but the recited example relates to the use of DES prior to encoding. Moreover, the reference to DES was in connection with emulating a random bit generator: "It is possible to use a block cipher like DES in combination with a sufficiently pseudo-random seed value to emulate a cryptographically secure random bit generator." Application at p. 18, lines 21-22.

encrypted data output that looks nothing like the input. DES does not involve hiding a watermark in independent data, but rather taking the independent data and modifying it to the point that it no longer resembles its initial appearance. Thus, there is no "mask set" in a DES cipher. Contrary to the Examiner's assertion, the key breakdown and permutations are simply data, and bear little relationship, if any, to the mask set claimed in the present application. Accordingly, Applicants traverse the Examiner's assertion that the "key breakdown and subsequent permutations correspond to applicant's mask set." *Id.*

Claims 40-51 rely on the use of a "mask set." Because Schneier fails to disclose or suggest the use of a mask set as disclosed in the claims (whether alone or in combination with the other references), and even fails to disclose the use of a stega-cipher, the rejections of claims 40-43 and 46-48 must be reversed. *See* MPEP 7.06.02(j) (the combined references must teach or suggest all claim limitations).

Claims 40-43 (which depend from independent claim 25) and claims 46-48 (which depend from independent claim 29) are also patentable over the combination because the combination fails to disclose the use of a "stega-cipher" as required by the claims. For at least this additional reason, the Examiner has failed to establish a prima facie case of obviousness, and thus the rejections of claims 40-43 and 46-48 must be reversed. *See* MPEP 7.06.02(j) (the combined references must teach or suggest all claim limitations).

E. Whether claims 52-57 are unpatentable under 35 U.S.C. § 103 over Powell in view of Barton.

1. Powell Cannot Properly Be Combined with Barton.

It is not readily apparent that there is a reasonable likelihood of success in combining the techniques of Barton with the techniques of Powell, at least as suggested by Examiner. In Powell, the pixel value (which is a luminance value) is adjusted a small positive or negative amount (preferably 2% to 10% of the initial pixel value), whereby the difference is indicative of a "1" or a "0". (Powell, page 4 lines 42-48). Hence, Powell teaches replacing a pixel value with a new value that is dependent upon the initial value (adjusted upwards or downwards 2-10%) of the pixel. The Examiner cites Barton in combination with Powell in two contexts (the use of "digital signatures," and the use of sequence data). It is not readily apparent how the "signature" of Powell or the "sequence data" of Powell could be combined with Barton, where the pixel

values are adjusted only a small positive or negative amount. Absent a clear way to implement the use of the "signature" or "sequence data" of Powell, there can be no likelihood of success in making the combination. Because the Examiner has failed to establish a motivating force and has failed to establish a reasonable likelihood of success, the rejection of claims 52-57 based on the combination of Powell and Barton must be reversed.

Furthermore, while both Powell and Barton reference a "signature," the meanings of these respective "signatures" are very different. Powell's signature is not a digital signature in a cryptographic sense, but rather is an image signature (*i.e.*, a visual pattern). (See Powell's background section wherein he says, "the existing digital signatures are unacceptable for use with digital images.") In accordance with Powell's own teachings, the digital signatures disclosed in Barton "are unacceptable for use with digital images." Thus, there is no motivation for combining Powell and Barton, and the rejections of claims 52-57 based on the combination of Powell and Barton must be reversed.

2. The Combination of Powell and Barton Does Not Disclose the Claimed Inventions.

The Examiner asserts that claims 52-57 are unpatentable over Powell in view of Barton.[7] Office Action dated Dec. 10, 2002, at ¶¶ 28-29.

With respect to claims 52-54, Examiner asserts:

> Powell et al. teach encrypting digital watermarks into information. They do not say that the watermarks are unique. In lines 20-33 of column 4, Barton teaches including sequence data with authentication data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to uniquely identify different samples so that the samples can be placed in the correct order. Unique watermarks could also deter cryptanalysis attacks.

Office Action dated Dec. 10, 2002, at ¶ 28.

With respect to claims 55-57, Examiner asserts:

> Powell et al. teach encrypting digital watermarks into information. They do not say that the data that is watermarked is hashed and attached to itself. Official notice is taken that hashing data and then attaching the hash to the data is

[7] U.S. Patent No. 5,912,972.

> old and well-known. The hash acts as verification. Digital signatures with message appendix are a common term implementation of this. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to attach a hash of the information to the information. This hash would be used to verify the integrity of the information.

Office Action dated Dec. 10, 2002, at ¶ 29.

As discussed above, Powell does not teach "encrypting digital watermarks into information with a key," and furthermore, does not teach the use of a stega-cipher for steganographically encoding watermarks into a carrier signal. The addition of Barton does not cure this shortcoming. For at least this reason, the combination does not yield the claimed invention, and accordingly, the 103 rejection of claims 52-57 must be reversed.

Claims 52-57 are allowable for the additional reason that the combination of Powell and Barton fails to yield another aspect of claim 52. Claim 52 relates to "adding unique data to each individual watermark, rendering it distinct from any other watermark in the same sample stream." Claim 52 requires that multiple watermarks exist in the same sample stream. The Examiner has not established where Powell (or Barton) teaches the use of multiple watermarks. Unless you have multiple watermarks, there is no need to consider marking them with unique data. Multiple watermarks may be governed by independent keys, which assist in creating uniqueness. Each encoding of a watermark may have a different strength level or different mapping location, or different random seed value, characteristics that are missing from the prior art.

The section of Barton cited by Examiner does not make obvious claims 52-57 for at least the additional reason that Barton fails to disclose "adding unique data to each individual watermark, rendering it distinct from any other watermark in the same sample stream":

> The invention provides a method and apparatus for basic authentication of a digital block and for carrying additional authentication information provided by the user, *i.e.* meta-data, in a secure and reliable fashion. To embed authentication data into a digital block, a digital signature is formed that is a reduced representation of the digital block. The signature and additional information supplied by the user are embedded into the digital block by replacing predetermined bits within the block. Encryption can be used to enhance authentication capability. The encrypted data can be further verified using error correction coding techniques. For sequential data, such as the frames of a video

> display, a sequence numbers can also be provided as part of the meta-data to ensure that frames have not been deleted or re-ordered.

U.S. Patent No. 5,912,972, Col. 4, lines 18-33. As understood, Barton encodes authentication information into a digital block by first making a digital signature of the digital block, adding meta-data provided by the user, and then encoding the digital signature and the meta data into the digital block. Barton further suggests that where the underlying data comprises sequential data such as video frames (for example, where the digital blocks represent video frames), the meta data being added can include frame numbers to indicate the sequence order. It would appear that the Examiner's argument has assumed that the meta-data represents a watermark (because it represents independent data provided by the user). The Examiner, however, is relying on the insertion of sequence information that directly relates to the underlying data. Thus, at best the Examiner's citation of Barton suggests that unique information about the underlying data can be added to the meta data to provide information about the underlying data. Claim 52 is directed to the unique identification of multiple watermarks that may be embedded into underlying data. Barton, at best, appears to teach the unique identification of the underlying data. The motivation for marking Barton's underlying data is based upon the purpose of the underlying data (*e.g.*, video frames). This motivation does not suggest any need or desire to uniquely mark the data that is being embedded into the underlying data. So, even assuming a motivation for combining Barton and Powell, the combination still does not disclose the invention of Claim 52, and therefore claim 52, and claims 53-57 that depend from claim 52, are not obvious. For at least this additional reason, the Board must reverse the rejection of Claims 52-57.

F. Whether claims 26, 30, and 52-57 are unpatentable under 35 U.S.C. § 103 over Bender in view of Barton.

1. The Combination of Bender and Barton Does Not Disclose the Claimed Inventions.

Examiner rejects claims 26, 30, 52-54, and 55-57 as unpatentable over Bender in view of Barton. *See* Office Action dated Dec. 10, 2002, at ¶¶ 30 and 38.

Claims 52-57 are allowable for at least the reason that the combination of Bender and Barton fails to yield the step of "adding unique data to each individual watermark, rendering it distinct from any other watermark in the same sample stream." Claim 52 requires that multiple watermarks exist in the same sample stream. The Examiner has not established where Bender

(or even Barton) teaches the use of multiple watermarks. Unless you have multiple watermarks, there is no need to consider marking them with unique data.

The section of Barton cited by Examiner does not make obvious claims 52-57 for at least the additional reason that Barton fails to disclose "adding unique data to each individual watermark, rendering it distinct from any other watermark in the same sample stream":

> The invention provides a method and apparatus for basic authentication of a digital block and for carrying additional authentication information provided by the user, *i.e.* meta-data, in a secure and reliable fashion. To embed authentication data into a digital block, a digital signature is formed that is a reduced representation of the digital block. The signature and additional information supplied by the user are embedded into the digital block by replacing predetermined bits within the block. Encryption can be used to enhance authentication capability. The encrypted data can be further verified using error correction coding techniques. For sequential data, such as the frames of a video display, a sequence numbers can also be provided as part of the meta-data to ensure that frames have not been deleted or re-ordered.

U.S. Patent No. 5,912,972, Col. 4, lines 18-33. As understood, Barton encodes authentication information into a digital block by first making a digital signature of the digital block, adding meta-data provided by the user, and then encoding the digital signature and the meta data into the digital block. Barton further suggests that where the underlying data comprises sequential data such as video frames (for example, where the digital blocks represent video frames), the meta data being added can include frame numbers to indicate the sequence order. It would appear that the Examiner's argument has assumed that the meta-data represents a watermark (because it represents independent data provided by the user). The Examiner, however, is relying on the insertion of sequence information that directly relates to the underlying data. Thus, at best the Examiner's citation of Barton suggests that unique information about the underlying data can be added to the meta data to provide information about the underlying data. Claim 52 is directed to the unique identification of multiple watermarks that may be embedded into underlying data. Barton, at best, appears to teach the unique identification of the underlying data. The motivation for marking Barton's underlying data is based upon the purpose of the underlying data (*e.g.*, video frames). This motivation does not suggest any need or desire to uniquely mark the data that is being embedded into the underlying data. So, even if you assume a motivation for combining Barton and Bender, you still do not have the invention of Claim 52, and therefore

claim 52, and claims 53-57 that depend from claim 52, are not obvious. Thus, the Board must reverse the rejection of Claims 52-57.

As discussed above, Bender does not teach "encrypting digital watermarks into information with a key," and furthermore, does not teach the use of a stega-cipher for steganographically encoding watermarks into a carrier signal. The addition of Barton does not cure this shortcoming. For at least this additional reason, the combination does not yield the claimed invention, and accordingly, the 103 rejection of claims 26, 30, 52-54, and 55-57 must be reversed.

CONCLUSION

For the reasons set forth above, Appellant respectfully requests that the Board reverse the final judgment of the Examiner and instruct the Examiner to issue a notice of allowance for the Claims 25-63 as last amended.

Respectfully submitted,

WILEY REIN & FIELDING LLP

Date: July 10, 2003

By: 

Floyd B. Chapman Reg. No. 40,555

WILEY REIN & FIELDING LLP
Attn: Patent Administration
1776 K Street, N.W.
Washington, D.C. 20006
Telephone: 202.719.7000
Facsimile: 202.719.7049

APPENDIX A

PENDING CLAIMS

25. A method for steganographically protecting a digital signal comprising the steps of:

a) providing a carrier signal

b) using a stega-cipher to steganographically encode independent information including a digital watermark into the carrier signal.

26. The method according to claim 25, wherein the carrier signal includes a stream of digital samples.

27. The method according to claim 25, wherein the carrier signal includes a continuous analog waveform.

28. The method according to claim 25, wherein the digital watermark, includes at least one selected from the group consisting of: rights ownership identification, authorship identification of the encoded carrier signal, ownership identification of a unique copy of the encoded carrier signal, and a serialization code uniquely identifying a copy of the encoded carrier signal.

29. A method for steganographically protecting a digital signal comprising:

a) providing a carrier signal that has been encoded with independent information; and

b) using a stega-cipher to steganographically decode independent information including a digital watermark from the carrier signal.

30. The method according to claim 29, wherein the carrier signal includes a stream of digital samples.

31. The method according to claim 29, wherein the carrier signal includes a continuous analog waveform.

32. The method according to claim 29, wherein the digital watermark includes at least one selected from the group consisting of: rights ownership identification, authorship identification of the encoded carrier signal, ownership identification of a unique copy of the encoded carrier signal, and a serialization code uniquely identifying a copy of the encoded carrier signal.

33. The method according to claim 29, further comprising the step of:

c) generating a first derivative encoded signal representing the original carrier signal combined with the encoded independent information, including the digital watermark, wherein the first derivative encoded signal is an arbitrarily close approximation of the original carrier signal.

34. The method according to claim 33, further comprising the step of:

d) modifying the first derivative encoded signal to produce a second derivative encoded signal, wherein the second derivative encoded signal differs from the original carrier signal by a greater degree than the first derivative encoded signal differs from the original carrier signal, as measured by an arbitrary signal metric.

35. The method according to claim 33, wherein the changes introduced to the original carrier signal in order to generate the first derivative encoded signal are chosen based on the random or pseudo-random key so that to erase or damage the watermark without using the random or pseudo-random key the first derivative encoded signal must be changed to produce a second derivative encoded signal, wherein the second derivative encoded signal differs from the original carrier signal by a greater degree than the first derivative encoded signal differs from the original carrier signal, as measured by an arbitrary signal metric.

36. The method according to claim 29, further comprising the step of:

c) decoding a single message bit from a single sample by reading a simple bit of the single sample as the message bit.

37. The method according to claim 29, further comprising the step of:

c) decoding a signal message bit from a single sample by mapping the single sample in the range of sample values which indicate a particular message bit value.

38. The method according to claim 29, further comprising the step of:

c) decoding a single message bit from a signal spectra value by mapping the single spectral into a range of sample values which indicate a particular message bit value.

39. The method according to claim 25, further comprising the step of:

c) using a map table to define where watermark information is to be encoded based on random or pseudo-random masks into the carrier signal, wherein the map table is defined such that any index of the map table enables encoding of information.

40. The method according to claim 25, further comprising the step of:

c) selecting a mask set, said mask stet including one or more random or pseudo-random series of bits, referred to as masks;

d) selecting a random or pseudo-random start of message delimiter; and

e) selecting independent information to be encoded.

41. The method according to claim 40, further comprising the step of:

f) generating a message bit stream to be encoded such that the stream includes:

1) the random or pseudo-random start of message delimiter;

2) a number of message bytes to follow the message; and

3) the independent information.

42. The method according to claim 41, further comprising the step of:

g) separating an input sample stream into smaller discrete sample windows comprising segments of the input sample stream.

43. The method according to claim 42, further comprising of the step of:

h) using positions within the sample windows and a position within the input stream to index random or pseudo-random masks and compute a mapping function to

determine encoding positions and encode digital watermark information into the sample windows.

44. The method according to claim 43, further comprising the step of:

i) computing a spectral transform of the sample windows prior to digital watermark data encoding.

45. The method according to claim 44, further comprising the step of:

j) computing an inverse spectral transform of the encoded spectral transform data after digital watermark data encoding.

46. The method according to claim 29, further comprising the steps of:

c) selecting a mask set, said mask set including one or more random or pseudo-random series of bits, referred to as masks,

d) selecting a random or pseudo-random start of message delimiter; and

e) selecting an input sample stream to be decoded.

47. The method according to claim 46, further comprising the step of:

f) separating the input sample stream into smaller discrete sample windows comprising segments of the input sample stream.

48. The method according to claim 47, further comprising the step of:

g) using positions within one of the sample windows and a position within the input stream to index random or pseudo-random masks and compute a mapping function to determine decoding positions and to decode digital watermark information from the sample window.

49. The method according to claim 48, further comprising the step of:

h) computing a spectral transform of the sample window prior to digital watermark data decoding.

50. The method according to claim 41, wherein the independent information contains, at least one selected from the group consisting of: a hash value computed on the start of message delimiter, and a digital signature of the start of message delimiter.

51. The method according to claim 48, further comprising the step of:

h) validating at least one selected from the group consisting of:

(1) a hash value computed on the start of message delimiter, and

(2) a digital signature of the start of message delimiter,

wherein the step h) of validating occurs after the start of message delimiter and the encoded information of said hash value or said digital signature have been decoded and the validation consists of computing an appropriate result using the start of message delimiter, comparing it to a value in the decoded data, and verifying any signature.

52. The method according to claim 25, further comprising the step of:

c) adding unique data to each individual watermark, rendering it distinct from any other watermark in the same sample stream.

53. The method according to claim 52, further comprising the step of:

d) pre-processing sample windows in the sample stream to be watermarked.

54. The method according to claim 53, further comprising the step of:

e) determining which sample windows will contain the individual digital watermark to be encoded.

55. The method according to claim 54, further comprising the step of:

f) calculating a size of the independent information comprising the digital watermark plus a size of an added hash value to determine a number of sample windows required to contain a complete watermark.

56. The method according to claim 55, further comprising the step of:

g) computing a secure one way hash function of the carrier signal data in said sample windows, wherein said hash function is insensitive to changes introduced into the carrier signal for the purpose of carrying digital watermark information.

57. The method according to claim 56, further comprising the step of:

h) concatenating the hash value with the independent information, creating an expanded, unique digital watermark.

58. The method according to claim 29, further comprising the step of:

c) obtaining a unique hash value contained in the independent information comprising part of the digital watermark.

59. The method according to claim 58, further comprising the additional step of:

d) re-processing sample windows in the sample stream which contained the decoded watermark.

60. The method according to claim 59, further comprising the step of:

e) computing a secure one way hash function of the carrier signal data in said sample windows, wherein said hash function is insensitive to changes introduced into the carrier signal for the purpose of carrying digital watermark information.

61. The method according to claim 60, further comprising the step of:

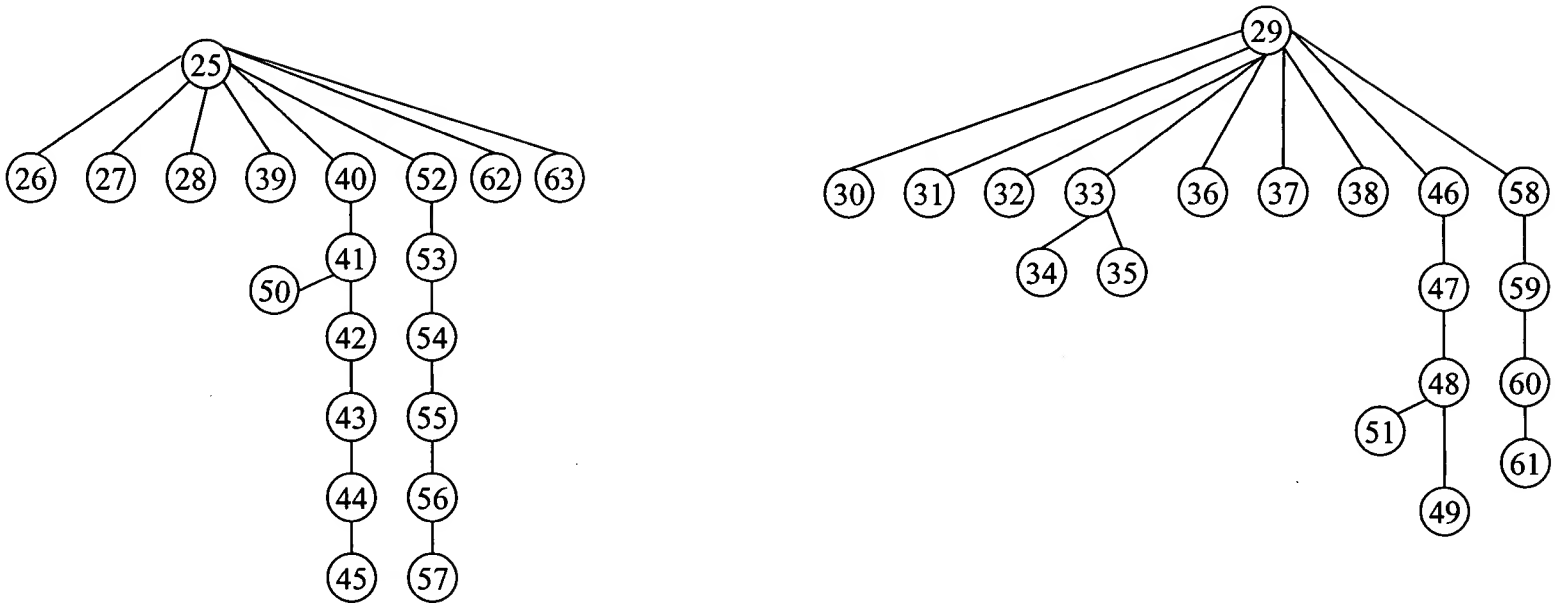
f) comparing the computed hash value to the value contained in the watermark.

62. The method of claim 25, wherein the step of steganographically encoding independent information into the carrier signal causes an imperceptible change in the carrier signal.

63. The method of claim 29, wherein the step of steganographically decoding independent information into the carrier signal causes an imperceptible change in the carrier signal.

APPENDIX B

Chart Showing Claim Dependencies
U.S. Patent Application Serial No. 08/999,766



CLAIM CHART FOR U.S. PATENT APPLICATION NO. 08/999,766
Title: STEGANOGRAPHIC METHOD AND DEVICE
Inventor: Scott Moskowitz, et al.

CLAIM ELEMENT	Bender 102	Powell 102	103	103
25. A method for steganographically protecting a digital signal comprising the steps of: a) providing a carrier signal b) using a stega-cipher to steganographically encode independent information including a digital watermark into the carrier signal.	Stega-cipher disclosed?	Stega-cipher disclosed?		
26. The method according to claim 25, wherein the carrier signal includes a stream of digital samples.		Stega-cipher disclosed?	Bender + Barton ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed?	
27. The method according to claim 25, wherein the carrier signal includes a continuous analog waveform.	Stega-cipher disclosed?	Stega-cipher disclosed?		

CLAIM CHART FOR U.S. PATENT APPLICATION NO. 08/999,766
Title: STEGANOGRAPHIC METHOD AND DEVICE
Inventor: Scott Moskowitz, et al.

CLAIM ELEMENT	Bender 102	Powell 102	103	103
28. The method according to claim 25, wherein the digital watermark, includes at least one selected from the group consisting of: rights ownership identification, authorship identification of the encoded carrier signal, ownership identification of a unique copy of the encoded carrier signal, and a serialization code uniquely identifying a copy of the encoded carrier signal.	Stega-cipher disclosed?	Stega-cipher disclosed?		
29. A method for steganographically protecting a digital signal comprising: a) providing a carrier signal that has been encoded with independent information; and b) using a stega-cipher to steganographically decode independent information including a digital watermark from the carrier signal.	Stega-cipher disclosed?	Stega-cipher disclosed?		
30. The method according to claim 29, wherein the carrier signal includes a stream of digital samples.		Stega-cipher disclosed?	Bender + Barton ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed?	

CLAIM CHART FOR U.S. PATENT APPLICATION NO. 08/999,766
Title: STEGANOGRAPHIC METHOD AND DEVICE
Inventor: Scott Moskowitz, et al.

CLAIM ELEMENT	Bender 102	Powell 102	103	103
31. The method according to claim 29, wherein the carrier signal includes a continuous analog waveform.	Stega-cipher disclosed?	Stega-cipher disclosed?		
32. The method according to claim 29, wherein the digital watermark includes at least one selected from the group consisting of: rights ownership identification, authorship identification of the encoded carrier signal, ownership identification of a unique copy of the encoded carrier signal, and a serialization code uniquely identifying a copy of the encoded carrier signal.	Stega-cipher disclosed?	Stega-cipher disclosed?		
33. The method according to claim 29, further comprising the step of: c) generating a first derivative encoded signal representing the original carrier signal combined with the encoded independent information, including the digital watermark, wherein the first derivative encoded signal is an arbitrarily close approximation of the original carrier signal.	Stega-cipher disclosed?	Stega-cipher disclosed?		

CLAIM CHART FOR U.S. PATENT APPLICATION NO. 08/999,766
Title: STEGANOGRAPHIC METHOD AND DEVICE
Inventor: Scott Moskowitz, et al.

CLAIM ELEMENT	Bender 102	Powell 102	103	103
34. The method according to claim 33, further comprising the step of: d) modifying the first derivative encoded signal to produce a second derivative encoded signal, wherein the second derivative encoded signal differs from the original carrier signal by a greater degree than the first derivative encoded signal differs from the original carrier signal, as measured by an arbitrary signal metric.			Powell + Schneier ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed?	Bender ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? 1st derivative encoded signal disclosed?
35. The method according to claim 33, wherein the changes introduced to the original carrier signal in order to generate the first derivative encoded signal are chosen based on the random or pseudo-random key so that to erase or damage the watermark without using the random or pseudo-random key the first derivative encoded signal must be changed to produce a second derivative encoded signal, wherein the second derivative encoded signal differs from the original carrier signal by a greater degree than the first derivative encoded signal differs from the original carrier signal, as measured by an arbitrary signal metric.	Stega-cipher disclosed?	Stega-cipher disclosed?		

CLAIM CHART FOR U.S. PATENT APPLICATION NO. 08/999,766
Title: STEGANOGRAPHIC METHOD AND DEVICE
Inventor: Scott Moskowitz, et al.

CLAIM ELEMENT	Bender 102	Powell 102	103	103
36. The method according to claim 29, further comprising the step of: c) decoding a single message bit from a single sample by reading a simple bit of the single sample as the message bit.		Stega-cipher disclosed?	Stega-cipher disclosed?	
37. The method according to claim 29, further comprising the step of: c) decoding a signal message bit from a single sample by mapping the single sample in the range of sample values which indicate a particular message bit value.		Stega-cipher disclosed?	Stega-cipher disclosed?	
38. The method according to claim 29, further comprising the step of: c) decoding a single message bit from a signal spectra value by mapping the single spectral into a range of sample values which indicate a particular message bit value.		Stega-cipher disclosed?	Stega-cipher disclosed?	
39. The method according to claim 25, further comprising the step of: c) using a map table to define where watermark information is to be encoded based on random or pseudo-random masks into the carrier signal, wherein the map table is defined such that any index of the map table enables encoding of information.		Stega-cipher disclosed?	Stega-cipher disclosed?	

CLAIM CHART FOR U.S. PATENT APPLICATION NO. 08/999,766
Title: STEGANOGRAPHIC METHOD AND DEVICE
Inventor: Scott Moskowitz, et al.

CLAIM ELEMENT	Bender 102	Powell 102	103	103
40. The method according to claim 25, further comprising the step of: c) selecting a mask set, said mask stet including one or more random or pseudo-random series of bits, referred to as masks; d) selecting a random or pseudo-random start of message delimiter; and e) selecting independent information to be encoded.			Powell + Schneier ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Mask set disclosed?	Bender + Schneier ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Mask set disclosed?

CLAIM CHART FOR U.S. PATENT APPLICATION NO. 08/999,766
Title: STEGANOGRAPHIC METHOD AND DEVICE
Inventor: Scott Moskowitz, et al.

CLAIM ELEMENT	Bender 102	Powell 102	103	103
41. The method according to claim 40, further comprising the step of: f) generating a message bit stream to be encoded such that the stream includes: 1) the random or pseudo-random start of message delimiter; 2) a number of message bytes to follow the message; and 3) the independent information.			Powell + Schneier ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Mask set disclosed?	Bender + Schneier ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Mask set disclosed?
42. The method according to claim 41, further comprising the step of: g) separating an input sample stream into smaller discrete sample windows comprising segments of the input sample stream.			Powell + Schneier ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Mask set disclosed?	Bender + Schneier ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Mask set disclosed?

CLAIM CHART FOR U.S. PATENT APPLICATION NO. 08/999,766
Title: STEGANOGRAPHIC METHOD AND DEVICE
Inventor: Scott Moskowitz, et al.

CLAIM ELEMENT	Bender 102	Powell 102	103	103
43. The method according to claim 42, further comprising of the step of: h) using positions within the sample windows and a position within the input stream to index random or pseudo-random masks and compute a mapping function to determine encoding positions and encode digital watermark information into the sample windows.			Powell + Schneier ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Mask set disclosed?	Bender + Schneier ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Mask set disclosed?
44. The method according to claim 43, further comprising the step of: i) computing a spectral transform of the sample windows prior to digital watermark data encoding.			Stega-cipher disclosed?	
45. The method according to claim 44, further comprising the step of: j) computing an inverse spectral transform of the encoded spectral transform data after digital watermark data encoding.			Stega-cipher disclosed?	

CLAIM CHART FOR U.S. PATENT APPLICATION NO. 08/999,766
Title: STEGANOGRAPHIC METHOD AND DEVICE
Inventor: Scott Moskowitz, et al.

CLAIM ELEMENT	Bender 102	Powell 102	103	103
46. The method according to claim 29, further comprising the steps of: c) selecting a mask set, said mask set including one or more random or pseudo-random series of bits, referred to as masks, d) selecting a random or pseudo-random start of message delimiter; and e) selecting an input sample stream to be decoded.			Powell + Schneier ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Mask set disclosed?	Bender + Schneier ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Mask set disclosed?
47. The method according to claim 46, further comprising the step of: f) separating the input sample stream into smaller discrete sample windows comprising segments of the input sample stream.			Powell + Schneier ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Mask set disclosed?	Bender + Schneier ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Mask set disclosed?

CLAIM CHART FOR U.S. PATENT APPLICATION NO. 08/999,766
Title: STEGANOGRAPHIC METHOD AND DEVICE
Inventor: Scott Moskowitz, et al.

CLAIM ELEMENT	Bender 102	Powell 102	103	103
48. The method according to claim 47, further comprising the step of: g) using positions within one of the sample windows and a position within the input stream to index random or pseudo-random masks and compute a mapping function to determine decoding positions and to decode digital watermark information from the sample window.			Powell + Schneier ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Mask set disclosed?	Bender + Schneier ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Mask set disclosed?
49. The method according to claim 48, further comprising the step of: h) computing a spectral transform of the sample window prior to digital watermark data decoding.			Stega-cipher disclosed?	
50. The method according to claim 41, wherein the independent information contains, at least one selected from the group consisting of: a hash value computed on the start of message delimiter, and a digital signature of the start of message delimiter.			Stega-cipher disclosed?	

CLAIM CHART FOR U.S. PATENT APPLICATION NO. 08/999,766
Title: STEGANOGRAPHIC METHOD AND DEVICE
Inventor: Scott Moskowitz, et al.

CLAIM ELEMENT	Bender 102	Powell 102	103	103
51. The method according to claim 48, further comprising the step of: h) validating at least one selected from the group consisting of: (1) a hash value computed on the start of message delimiter, and (2) a digital signature of the start of message delimiter, wherein the step h) of validating occurs after the start of message delimiter and the encoded information of said hash value or said digital signature have been decoded and the validation consists of computing an appropriate result using the start of message delimiter, comparing it to a value in the decoded data, and verifying any signature.			Stega-cipher disclosed?	
52. The method according to claim 25, further comprising the step of: c) adding unique data to each individual watermark, rendering it distinct from any other watermark in the same sample stream.			Powell + Barton ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Unique data for each watermark disclosed?	Bender + Barton ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Unique data for each watermark disclosed?

CLAIM CHART FOR U.S. PATENT APPLICATION NO. 08/999,766
Title: STEGANOGRAPHIC METHOD AND DEVICE
Inventor: Scott Moskowitz, et al.

CLAIM ELEMENT	Bender 102	Powell 102	103	103
53. The method according to claim 52, further comprising the step of: d) pre-processing sample windows in the sample stream to be watermarked.			Powell + Barton ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Unique data for each watermark disclosed?	Bender + Barton ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Unique data for each watermark disclosed?
54. The method according to claim 53, further comprising the step of: e) determining which sample windows will contain the individual digital watermark to be encoded.			Powell + Barton ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Unique data for each watermark disclosed?	Bender + Barton ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Unique data for each watermark disclosed?

CLAIM CHART FOR U.S. PATENT APPLICATION NO. 08/999,766
Title: STEGANOGRAPHIC METHOD AND DEVICE
Inventor: Scott Moskowitz, et al.

CLAIM ELEMENT	Bender 102	Powell 102	103	103
55. The method according to claim 54, further comprising the step of: f) calculating a size of the independent information comprising the digital watermark plus a size of an added hash value to determine a number of sample windows required to contain a complete watermark.			Powell + Barton ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Unique data for each watermark disclosed?	Bender + Barton ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Unique data for each watermark disclosed?
56. The method according to claim 55, further comprising the step of: g) computing a secure one way hash function of the carrier signal data in said sample windows, wherein said hash function is insensitive to changes introduced into the carrier signal for the purpose of carrying digital watermark information.			Powell + Barton ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Unique data for each watermark disclosed?	Bender + Barton ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Unique data for each watermark disclosed?

CLAIM CHART FOR U.S. PATENT APPLICATION NO. 08/999,766
Title: STEGANOGRAPHIC METHOD AND DEVICE
Inventor: Scott Moskowitz, et al.

CLAIM ELEMENT	Bender 102	Powell 102	103	103
57. The method according to claim 56, further comprising the step of: h) concatenating the hash value with the independent information, creating an expanded, unique digital watermark.			Powell + Barton ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Unique data for each watermark disclosed?	Bender + Barton ☐ Is there motivation to combine? ☐ Does combination yield all elements? Stega-cipher disclosed? Unique data for each watermark disclosed?
58. The method according to claim 29, further comprising the step of: c) obtaining a unique hash value contained in the independent information comprising part of the digital watermark.			Stega-cipher disclosed?	
59. The method according to claim 58, further comprising the additional step of: d) re-processing sample windows in the sample stream which contained the decoded watermark.			Stega-cipher disclosed?	

CLAIM ELEMENT	Bender 102	Powell 102	103	103
60. The method according to claim 59, further comprising the step of: e) computing a secure one way hash function of the carrier signal data in said sample windows, wherein said hash function is insensitive to changes introduced into the carrier signal for the purpose of carrying digital watermark information.			Stega-cipher disclosed?	
61. The method according to claim 60, further comprising the step of: f) comparing the computed hash value to the value contained in the watermark.			Stega-cipher disclosed?	
62. The method of claim 25, wherein the step of steganographically encoding independent information into the carrier signal causes an imperceptible change in the carrier signal.	Stega-cipher disclosed?	Stega-cipher disclosed?		
63. The method of claim 29, wherein the step of steganographically decoding independent information into the carrier signal causes an imperceptible change in the carrier signal.	Stega-cipher disclosed?	Stega-cipher disclosed?		